

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-122681  
 (43)Date of publication of application : 30.04.1999

(51)Int.CI. H04Q 9/00  
 H04Q 9/00  
 H04B 7/24  
 H04L 9/08  
 H04L 12/28

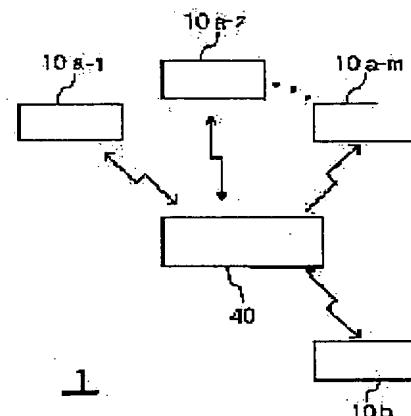
(21)Application number : 09-282329 (71)Applicant : SONY CORP  
 (22)Date of filing : 15.10.1997 (72)Inventor : MAEKAWA TAKUJI

## (54) RADIO SYSTEM, RADIO SYSTEM MANAGEMENT DEVICE, AND RADIO TERMINAL EQUIPMENT

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a radio system where a terminal equipment used in each home is not connected by mistake to an adjacent home or a network to which the terminal equipment does not belong or is not used by another person but is connected properly only to the connect network and is properly in use.

**SOLUTION:** In the case of connecting a terminal equipment 10b whose access right is not permitted yet to a network, at first the terminal equipment 10b sends a joining request signal to join in the network to a management device 40. The management device 40 receiving the joining request signal sends a signal of requesting transmission of key data to the terminal equipment 10b. The terminal equipment 10b receiving the transmission request signal of key data reads key data stored in a key storage section in the terminal equipment 10b and sends the data to the management equipment 40. The management equipment 40 calculates based on the received key data to discriminate whether or not encryption data stored in advance are decoded. As a result when the data are decoded, the equipment 40 conducts processing of giving an access right to the terminal equipment 10b.



### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

[application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's  
decision of rejection]  
[Date of requesting appeal against  
examiner's decision of rejection]  
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-122681

(43)公開日 平成11年(1999)4月30日

| (51)Int.Cl. <sup>6</sup> | 識別記号  | F I         |         |
|--------------------------|-------|-------------|---------|
| H 04 Q 9/00              | 3 2 1 | H 04 Q 9/00 | 3 2 1 B |
|                          | 3 1 1 |             | 3 1 1 A |
| H 04 B 7/24              |       | H 04 B 7/24 | E       |
| H 04 L 9/08              |       | H 04 L 9/00 | 6 0 1 E |
| 12/28                    |       | 11/00       | 3 1 0 Z |

審査請求 未請求 請求項の数 8 OL (全 9 頁)

(21)出願番号 特願平9-282329

(71)出願人 000002185

(22)出願日 平成9年(1997)10月15日

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 前川 卓司

東京都品川区北品川6丁目7番35号 ソニー株式会社内

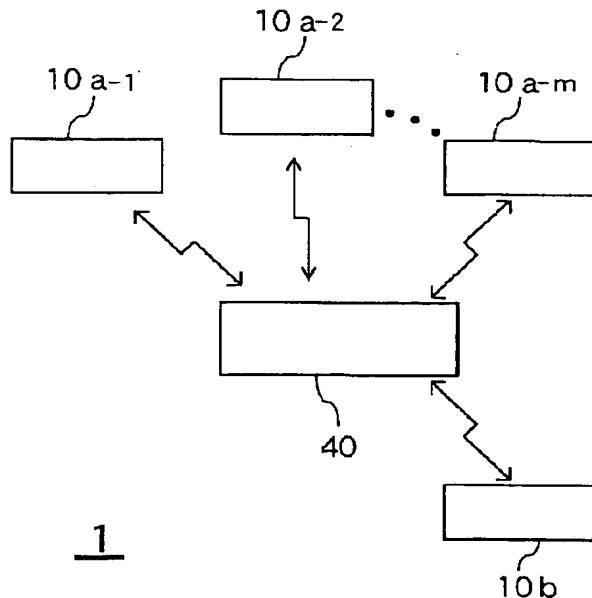
(74)代理人 弁理士 佐藤 隆久

(54)【発明の名称】 無線システム、無線システム管理装置および無線端末装置

(57)【要約】

【課題】通常の通信機能を有する家庭用装置を用いたのでは、隣接するネットワークとの混信などがあり適切な家庭内無線システムを構築できない。

【解決手段】未だアクセス権を許可していない端末装置10bをネットワークに接続する時には、まず端末装置10bは、管理装置40に対してネットワークへの加入要求信号を送信する。この加入要求信号を受信した管理装置40は、端末装置10bに対して鍵データの送信を要求する信号を送信する。この鍵データの送信要求信号を受信した端末装置10bは、端末装置10b内の鍵記憶部に記憶されている鍵データを読み出し、管理装置40に送信する。管理装置40は、この送信された鍵データにより前述したような計算を行い、予め記憶している暗号データを解くことができるか否かを判別する。その結果、解くことができた場合に、端末装置10bにアクセス権を与える処理を行う。



## 【特許請求の範囲】

【請求項1】特定の小領域内に配置された装置が、無線により任意に実質的に接続される無線システムであつて、

予め設定された所定の装置であつて、当該無線システムを特定する所定の識別番号を各々有する1以上の端末装置と、

当該無線システムに対する前記端末装置の接続を管理する管理装置であつて、当該無線システムに接続を要求している装置より前記識別番号を獲得し、該識別番号に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定し、該判定結果に基づいて当該装置の前記無線システムへの接続を制御する無線システム管理装置とを有する無線システム。

【請求項2】前記所定の識別番号は、所定の鍵データであり、

前記無線システム管理装置は、前記装置より前記鍵データを獲得し、当該鍵データ、および、予め無線システム管理装置に設定されている所定の暗号データに基づいて所定の演算を行い、該演算結果に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定する請求項1記載の無線システム。

【請求項3】前記端末装置の前記鍵データ、および、前記無線システム管理装置の前記暗号データは、任意に変更可能である請求項2記載の無線システム。

【請求項4】前記小領域は家庭であつて、家庭内の任意の装置を無線により任意に実質的に接続させる請求項3記載の無線システム。

【請求項5】特定の小領域内に配置された装置が無線により任意に実質的に接続される無線システムに対する前記端末装置の接続を管理する管理装置であつて、

当該無線システムに接続を要求している装置より前記識別番号を獲得する識別番号獲得手段と、

前記獲得した識別番号に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定する判定手段と、

前記判定結果に基づいて当該装置の前記無線システムへの接続を制御する接続制御手段とを有する無線システム管理装置。

【請求項6】前記所定の識別番号は、所定の鍵データであり、

前記識別番号獲得手段は、前記装置より前記鍵データを獲得し、

前記判定手段は、前記鍵データ、および、予め無線システム管理装置に設定されている所定の暗号データに基づいて所定の演算を行い、該演算結果に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定する請求項5記載の無線システム管理装置。

【請求項7】無線により所定の無線システムに接続され

る装置であつて、

前記接続される無線システムを特定する所定の識別番号を入力する識別番号入力手段と、

当該入力された識別番号を記憶する識別番号記憶手段と、

要求に応じて、当該識別番号を出力する識別番号出力手段とを有する無線端末装置。

【請求項8】前記識別番号入力手段は、当該端末装置とは分離可能なりモートコントロール装置である請求項7記載の無線端末装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、たとえば家庭などの中で、無線により複数の装置が通信を行いながら所定の処理を行うような無線システム、および、その無線システムに用いられる無線システム管理装置および無線端末装置に関する。

## 【0002】

【従来の技術】たとえば通信技術の進展などにより、家庭内で用いられる種々の電子機器においても無線装置により駆動され、また他の装置と通信を行いながら所定の機能を実現するような機器が増えている。たとえば、テレビジョン受像機やビデオテープレコーダなどはリモートコントローラ（リモコン）により操作されるのが普通になっているし、コードレス電話や携帯型の電話器、ページャ装置などの無線式の通信装置の普及も著しい。さらに、近年のネットワーク技術の急速な発展により、いわゆる家電製品から通信機器、パーソナルコンピュータなどの各装置をより密接に接続し、有効に利用しようという家庭内ネットワークも実現されつつある。

## 【0003】

【発明が解決しようとする課題】しかしながら、これまでの家庭用電気機器を用いたのでは、そのような家庭内ネットワークを構築しようとした場合に、適切に行えないという問題がある。そのような家庭内ネットワークは、通常、比較的近接して位置に多数のネットワークが存在することになっている。そして、これまでの通常の家庭用電気機器では、使用する周波数帯や通信手順などを変えて、確率的に同一の装置同士が近接した位置で用いられないようになっている場合が多い。そのため、偶然同じ装置が近接した位置で用いられたり、あるいは、意図的にそのような装置が作成されたような場合には、たとえば自分の家の装置が他の家庭のネットワークに接続されたり他の人に使用されてしまったり、隣の家庭の装置を自分の家のネットワークに接続してしまったりという問題が生じる。具体的には、伝送内容が装置を操作するようなものであれば、たとえばネットワークに接続された装置を適切に操作することができなくなるという問題が生じる。また、伝送内容が人間同士の対話に関するようなものであれば、その内容を傍受されてプライバシ

一が保護されないという問題が生じる。

【0004】したがって本発明の目的は、各家庭で使用される端末装置が、たとえば隣の家庭、あるいは、本来属していないようなネットワークにより誤って接続されたり、他の人により使用されたりすることがなく、本来のネットワークにのみ適切に接続されて適切に使用されるような無線システムを提供することにある。また本発明の他の目的は、そのような無線システムを構築するための無線システム管理装置を提供することにある。さらに本発明の他の目的は、そのような無線システムを構築するための無線端末装置を提供することにある。

【0005】

【課題を解決するための手段】したがって、本発明の無線システムは、特定の小領域内に配置された装置が、無線により任意に実質的に接続される無線システムであって、予め設定された所定の装置であって、当該無線システムを特定する所定の識別番号を各々有する1以上の端末装置と、当該無線システムに対する前記端末装置の接続を管理する管理装置であって、当該無線システムに接続を要求している装置より前記識別番号を獲得し、該識別番号に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定し、該判定結果に基づいて当該装置の前記無線システムへの接続を制御する無線システム管理装置とを有する。

【0006】好適には、前記所定の識別番号は、所定の鍵データであり、前記無線システム管理装置は、前記装置より前記鍵データを獲得し、当該鍵データ、および、予め無線システム管理装置に設定されている所定の暗号データに基づいて所定の演算を行い、該演算結果に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定する。また好適には、前記端末装置の前記鍵データ、および、前記無線システム管理装置の前記暗号データは、任意に変更可能である。特定的には、前記小領域は家庭であって、家庭内の任意の装置を無線により任意に実質的に接続させる。

【0007】また、本発明の無線システム管理装置は、特定の小領域内に配置された装置が無線により任意に実質的に接続される無線システムに対する前記端末装置の接続を管理する管理装置であって、当該無線システムに接続を要求している装置より前記識別番号を獲得する識別番号獲得手段と、前記獲得した識別番号に基づいて当該装置が当該無線システムに属する前記予め設定された所定の装置であるか否かを判定する判定手段と、前記判定結果に基づいて当該装置の前記無線システムへの接続を制御する接続制御手段とを有する。好適には、前記所定の識別番号は、所定の鍵データであり、前記識別番号獲得手段は、前記装置より前記鍵データを獲得し、前記判定手段は、前記鍵データ、および、予め無線システム管理装置に設定されている所定の暗号データに基づいて所定の演算を行い、該演算結果に基づいて当該装置が当

該無線システムに属する前記予め設定された所定の装置であるか否かを判定する。

【0008】また、本発明の無線端末装置は、無線により所定の無線システムに接続される装置であって、前記接続される無線システムを特定する所定の識別番号を入力する識別番号入力手段と、当該入力された識別番号を記憶する識別番号記憶手段と、要求に応じて、当該識別番号を出力する識別番号出力手段とを有する。特定的には、前記識別番号入力手段は、当該端末装置とは分離可能なリモートコントロール装置である。

【0009】

【発明の実施の形態】本発明の一実施の形態を図1～図6を参照して説明する。本実施の形態においては、家庭において用いられる、たとえばビデオテープレコーダ、テレビジョン受信機、ホームオートメーション機器、ホームテレフォン、および、外部との通信端末である電話機や有線放送端末などの、各種の複数の機器が、必要に応じて適宜無線により通信を行いながら、各々所望の動作を行う家庭内無線システムについて説明する。なおこれらの各機器は、各々が独自の機能を有し独自の動作を行うものであるが、ここでは、本発明に係わり、それら各機器間の通信方法について説明する。すなわち、各機器について、それが実際には何の装置であるかについては示さず、その通信部についてのみ説明する。

【0010】図1は、その家庭内無線システム1の構成を模式的に示す図である。家庭内無線システム1は、複数の端末装置10a<sub>1</sub>～10a<sub>n</sub>、10bと、1台の管理装置40とを有する。なお、これらの端末装置10a<sub>1</sub>～10a<sub>n</sub>および管理装置40は、各々、前述したような家庭内で用いられる機器である。図1において、端末装置10a<sub>1</sub>～10a<sub>n</sub>は既に管理装置40によりアクセス権が認可されている端末装置であり、端末装置10bは、未だアクセス権が認可されていない端末装置である。以後、所定の暗号データおよび鍵データを用いることにより、この端末装置10bに対してアクセス権が認可される処理を主に説明することにより、本発明について説明する。

【0011】まず、その端末装置10a<sub>1</sub>～10a<sub>n</sub>、10bの構成および動作について図2を参照して説明する。なお、端末装置10a<sub>1</sub>～10a<sub>n</sub>、10bは、実質的に同一の構成を有するものであるが、ここでは端末装置10bを用いてこれら端末装置について説明する。

図2は、その端末装置10bの本発明に係わる主要部の構成を示すブロック図である。端末装置10bは、信号受信部11、アンプ(AMP)12、書き込み部13、暗号データ記憶部14、鍵データ記憶部15、読み出し部16、符号器17、変調器18、デジタル/アナログ(D/A)変換部19および信号送信部20を有する。

【0012】なお、端末装置10bは図示せぬ制御部を有しており、この制御部により、端末装置10bが全体

として所望の動作を行うように、端末装置10bの各部が制御される。また、端末装置10bは、図3に示すよる、本体とは分離して用いられ、数字の0~9を入力可能なりモート・コントローラ30を有する。端末装置10bの使用者は、このリモート・コントローラ30を介して端末装置10bに対して暗号データおよび鍵データの設定を行う。

【0013】信号受信部11は、リモート・コントローラ30より送信される暗号データおよび鍵データを示す信号を受信する。信号受信部11は、フォト・トランジスタを有しており、これによりリモート・コントローラ30より送信されるたとえば赤外線などの信号を受信し、電気信号を生成してアンプ12に出力する。アンプ12は、信号受信部11で生成された暗号データおよび鍵データである電気信号を、後段の信号処理部で処理可能なレベルまで増幅し、増幅した信号を書き込み部13に出力する。書き込み部13は、アンプ12で増幅された信号の暗号データを暗号記憶部14に、鍵データを鍵記憶部15に各々記憶する。

【0014】暗号データ記憶部14は、書き込み部13より入力された暗号データを記憶する。暗号データ記憶部14は、不揮発性メモリで構成されており、電源が切れても記憶されたデータは抹消されない。鍵データ記憶部15は、書き込み部13より入力された鍵データを記憶する。鍵データ記憶部15も、暗号データ記憶部14と同様に、不揮発性メモリで構成されており、電源が切れても記憶されたデータは抹消されない。読み出し部16は、暗号データ記憶部14および鍵データ記憶部15に記憶されている暗号データおよび鍵データを適宜読み出し、符号器17に出力する。

【0015】符号器17は、たとえば読み出し部16より読み出された暗号データおよび鍵データなどの管理装置40に対して送信するデータを符号化し、変調器18に出力する。変調器18は、符号器17で符号化された送信データを、各々送信するのに適した信号に変調し、D/A変換部19に出力する。D/A変換部19は、変調器18で変調された送信信号をデジタル/アナログ変換し、実際に送信を行うための信号を生成し、信号送信部20に印加する。信号送信部20は、アンテナであり、D/A変換部19より印加された信号を出力し、管理装置40に対して所望のデータを送信する。

【0016】このような構成の端末装置10bにおいては、リモート・コントローラ30からの暗号データと鍵データの信号は、信号受信部11によって検出され、アンプ12で増幅され、書き込み部13を介して各々暗号データ記憶部14および鍵データ記憶部15に記憶される。鍵データ記憶部15に記憶された鍵データは、読み出し部16により読み出され、符号器17により符号化され、変調器18により変調され、D/A変換部19によりアナログ信号に変調され、信号送信部20によりネ

ットワークを管理する管理装置40に対して送信される。

【0017】次に、管理装置40の構成および動作について図4を参照して説明する。図4は、その管理装置40の構成を示すブロック図である。管理装置40は、信号受信部41、アナログ/デジタル(A/D)変換部42、復調器43、復号器44、書き込み部45、第1の記録部46、第1の読み出し部47、第2の記録部48、第2の読み出し部49、鍵識別部50、符号器51、変調器52、デジタル/アナログ(D/A)変換部53および信号送信部54を有する。なお、管理装置40は図示せぬ制御部を有しており、この制御部により、管理装置40が全体として所望の動作を行うように、管理装置40の各部が制御される。

【0018】信号受信部41は、アンテナであり、家庭内無線システム1内の端末装置10a<sub>1</sub>~10a<sub>n</sub>や、家庭内無線システム1に属さない端末装置10bなどから送信される種々の信号を受信し、受信した信号に応じた電気信号を生成してA/D変換部42に出力する。A/D変換部42は、信号受信部41より入力される受信信号をデジタル信号に変換し、復調器43に出力する。復調器43は、A/D変換部42より入力される受信信号を復調してベースバンド信号を生成し、復号器44に出力する。

【0019】復号器44は、復調器43より入力された復調された信号を復号化し、元のデータを再生する。この再生した信号は、図示せぬ管理装置40の制御部に出力され、データの種類によっては、その制御部の指示により書き込み部45に出力される。具体的には、たとえば端末装置10bなどから家庭内無線システム1への加入要求が送信してきた場合などには、その信号は制御部に出力されるだけである。また、鍵データが送信してきた場合などには、その信号は制御部に出力されるとともに、第1の記録部46に記録されるために、制御部の指示により書き込み部45にも出力される。

【0020】第1の記録部46は、管理装置40に送信された鍵データなどを記憶する記憶部であり、半導体メモリなどにより構成される。第1の読み出し部47は、第1の記録部46に記憶されているたとえば鍵データを適宜読み出し、鍵識別部50に出力する。第2の記録部48は、予め管理装置40に設定された暗号データなどが記憶されている記憶部であり、電源が切れても記憶されたデータは抹消されないように、たとえば不揮発性メモリで構成されている。第2の読み出し部49は、第2の記録部48に記憶されているたとえば暗号データを適宜読み出し、鍵識別部50に出力する。

【0021】鍵識別部50は、第1の読み出し部47より入力される鍵データと、第2の読み出し部49より入力される暗号データに基づいて、その鍵データと暗号データが対応するものか否かを判定する。鍵識別部50

は、その判定結果を制御部に出力するとともに、それらが対応するデータであった場合にはアクセス権を認可する信号を、またそれらが対応しないデータであった場合にはアクセス権を認可しない信号を各々符号器51に出力する。

【0022】符号器51は、鍵識別部50または図示せぬ管理装置40の制御部から入力される送信用の信号を符号化し、変調器52に出力する。変調器52は、符号器51より入力される符号化された送信信号を送信に適した信号に変調し、デジタル／アナログ変換部53に出力する。D/A変換部53は、変調器52で変調された信号をデジタル／アナログ変換し、実際に送信を行うための信号を生成し、信号送信部54に印加する。信号送信部54は、実際にはアンテナであり、D/A変換部53より印加されたたとえば端末装置10bに送信するための信号を出力する。

【0023】このような構成の管理装置40における、本発明に係わる動作について図5を参照して説明する。図5は、管理装置40の動作を示すフローチャートである。なお、図5に示すフローチャートにおいて、条件の判断やそれに基づく実際の処理の指示は、管理装置40の図示せぬ制御部が行う。管理装置40は、まず動作が開始されると（ステップS0）、たとえば端末装置10bのような、アクセス権を保持していない端末からの家庭内無線システム1への加入要求信号が来ているか否かをチェックする（ステップS1）。加入要求信号が来ていない場合には、所定時間ウェイティングした後（ステップS2）、ステップS1に戻り引き続き加入要求信号の検出処理を行う。

【0024】ステップS1において、加入要求信号が検出されたら、その信号を送信した端末装置10bに対して鍵データを要求する信号を送信し（ステップS3）、鍵データを受信したか否かをチェックを行う（ステップS4）。鍵データを受信できていない間は、適宜ステップS3に戻り鍵データを要求する信号を繰り返し送信す

$$Y_a = g^{ka} \pmod{N} = 23^{41} \pmod{47} = 15 \quad \dots (1)$$

$$K = Y_b^{ka} \pmod{N} = 32^{41} \pmod{47} = 12 \quad \dots (2)$$

【0029】

$$Y_b = g^{kb} \pmod{N} = 23^{18} \pmod{47} = 32 \quad \dots (3)$$

$$K = Y_a^{kb} \pmod{N} = 23^{18} \pmod{47} = 12 \quad \dots (4)$$

【0030】家庭内無線システム1の管理装置40では、このような計算を行うことにより、端末装置10bが家庭内無線システム1内の装置か否か、すなわちアクセス権を許可してよい端末装置か否かを判定する。すなわち、管理装置40は、アクセス権を持たない端末に、この鍵Kbの送信を要求し、送信されてきた鍵Kbを用いて式(1)と(2)、および、式(3)と(4)を各々計算してその結果を比較する。その結果、同じKの値が導きだされた場合には、家庭内無線システム1に属する端末からのアクセス権の認可要求と考えて、管理装置

る（ステップS3）。鍵データを受信したら、前述したように、その鍵データを信号受信部41～書き込み部45を介してその鍵データを第1の記録部46に記録する（ステップS5）。

【0025】次に、その記録した鍵データを第1の記録部46より第1の読み出し部47を介して鍵識別部50に読み出し（ステップS6）、また予め第2の記録部48に記録されている暗号データを第2の読み出し部49を介して鍵識別部50に読み出す（ステップS7）。そして、鍵識別部50においてその読み出した鍵データで暗号データを解く処理を行い、暗号が解けた場合には、鍵識別部50～信号送信部54によりアクセス権を許可する信号を端末装置10bに送信し（ステップS9）、一連の処理を終了する（ステップS11）。また、ステップS8において、読み出した鍵データで暗号データを解けなかった場合には、鍵識別部50～信号送信部54によりアクセス権を不許可する信号を端末装置10bに送信し（ステップS10）、処理を終了する（ステップS11）。

【0026】ここで、本実施の形態で用いる暗号データと鍵データについて説明する。本実施の形態においては、Diffie & Hellman方式の暗号と鍵の処理を用いるものとする。この方式においては、家庭内無線システム1内に属する装置の全て、すなわち端末装置10a-1～10a-n、10bと管理装置40の全ての装置に、素数Nとその母数から導き出される値g(finite field)を入力しておく。具体例として、N=47に基づく値g=23を設定しておくとする。そして、各々正の整数である暗号Kaと、鍵Kbを、各々管理装置40および端末装置10a-1～10a-n、10bに設定しておく。

【0027】これらの値g、Ka、Kbを用いて、式(1)と(2)、および、式(3)と(4)を計算すると、どちらも同じ計算結果K=12を得る。

【0028】

【数1】

$$Y_a = g^{ka} \pmod{N} = 23^{41} \pmod{47} = 15 \quad \dots (1)$$

$$K = Y_b^{ka} \pmod{N} = 32^{41} \pmod{47} = 12 \quad \dots (2)$$

【数2】

$$Y_b = g^{kb} \pmod{N} = 23^{18} \pmod{47} = 32 \quad \dots (3)$$

$$K = Y_a^{kb} \pmod{N} = 23^{18} \pmod{47} = 12 \quad \dots (4)$$

40は端末装置10bにアクセス権を許可する。

【0031】次に、このような、端末装置10a-1～10a-n、10bおよび管理装置40を有する家庭内無線システム1において、アクセス権が許可されていない端末装置10bがアクセス権を得る処理について説明する。まず、新しい端末を家庭内無線システム1に加入する際には、予め、図3に示したようなりモート・コントローラ30により、0～9の数字の組み合わせとして作成された暗号と鍵を、その端末装置に設定しておく。この時、最初に入力された数字の組み合わせが暗号とし

て、また、次に入力される数字の組み合わせがそれを解くための鍵として記録される。

【0032】そして、ネットワークを初期化した時や、新しい端末あるいは未だアクセス権を許可していない端末をネットワークに子ノードとして認識させたい時などで、端末装置10bが実際にアクセス権の許可を求める時には、まず、端末装置10bは、管理装置40に対してネットワークへの加入要求信号を送信する。この加入要求信号を受信した管理装置40は、端末装置10bに対して鍵データの送信を要求する信号を送信する。この鍵データの送信要求信号を受信した端末装置10bは、端末装置10b内の鍵記憶部15に記憶されている鍵データを読み出し、管理装置40に送信する。

【0033】管理装置40は、この送信された鍵データにより前述したような計算を行い、第2の記録部48に記憶されている暗号データを解くことができるか否かを判別する。その結果、解くことができた場合に、端末装置10bにアクセス権を与える処理を行い、解くことができなかっ場合には、アクセス権の付与を行わない。このような、管理装置40と端末装置10bとの間の信号の送受の状態を図6に示す。なお、一度家庭内無線システム1によって認識された端末装置は、その後、鍵のやりとり等の処理を行うことなく、家庭内無線システム1内での任意の装置間でのアクセスを行うことができる。

【0034】このように、本実施の形態の家庭内無線システム1においては、家庭内無線システム1内の各端末に共通の鍵を持たせて、この鍵により通信可能な端末装置を選択して、有効なネットワークトポロジーを決定している。したがって、家庭内無線システム1に属さず共通の鍵を持っていない端末装置は、たとえ通信周波数や通信手順などが同一であっても、家庭内無線システム1に誤って認識されることがなくなる。その結果、共通の鍵を持たない端末装置による家庭内無線システム1への不正なアクセスを防ぐことができる。また、誤った端末装置と通信を行うことにより、各装置が誤動作することなどを防ぐことができる。また、本実施の形態の家庭内無線システム1においては、鍵は任意に決定することができるので、定期的に、あるいは、必要に応じて適宜変更すれば、より信頼性の高い家庭内無線システム1を構築することができる。

【0035】なお、本発明は、本実施例に限るものではなく、任意好適な種々の改変が可能である。たとえば、本実施の形態においては、家庭内における無線システムを例示したが、このようなシステムに限られるものではなく、任意のネットワークに適用可能である。

【0036】

【発明の効果】以上説明したように、本発明によれば、共通の鍵を持たない端末装置による無線ネットワークへの不正なアクセスを防ぐことができ、誤った端末装置と通信を行うことによる誤動作することなどを防ぐことができる。その結果、本来のネットワークにのみ適切に接続されて適切に使用されるような無線システム、その無線システムに用いられる無線システム管理装置、および、そのような無線システムを構築することのできる無線端末装置を提供することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態の家庭内無線システムの構成を示す図である。

【図2】図1に示した家庭内無線システムの端末装置の構成を示す図である。

【図3】図2に示した端末装置のリモート・コントローラを示す図である。

【図4】図1に示した家庭内無線システムの管理装置の構成を示す図である。

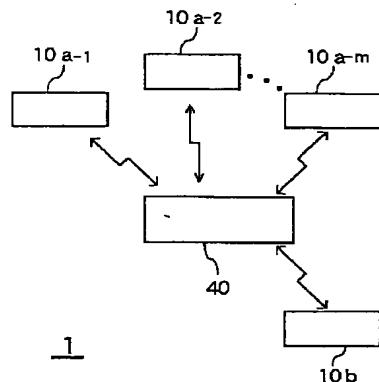
【図5】図4に示した管理装置の動作を説明するためのフローチャートである。

【図6】家庭内無線システムにおいて、新規加入を要求する端末装置と管理装置との間の信号の送受信の状態を示す図である。

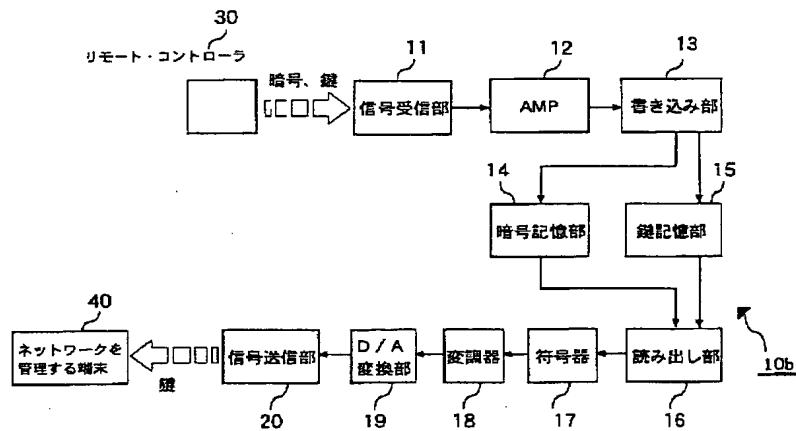
【符号の説明】

1…家庭内無線システム、10…端末装置、11…信号受信部、12…アンプ、13…書き込み部、14…暗号記憶部、15…鍵記憶部、16…読み出し部、17…符号器、18…変調器、19…デジタル／アナログ(D/A)変換部、20…信号送信部、40…管理装置、41…信号受信部、42…A/D変換部、43…復調器、44…復号器、45…書き込み部、46…第1の記録部、47…第1の読み出し部、48…第2の記録部、49…第2の読み出し部、50…鍵識別部、51…符号器、52…変調器、53…デジタル／アナログ(D/A)変換部、54…信号送信部

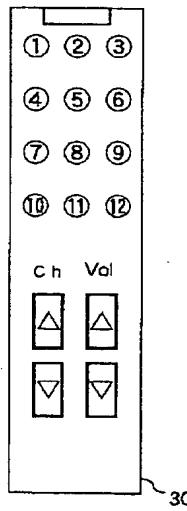
【図1】



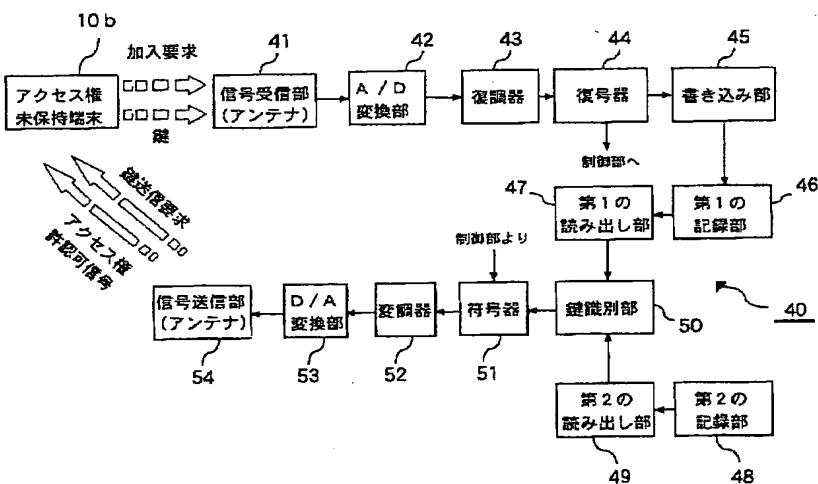
【図2】



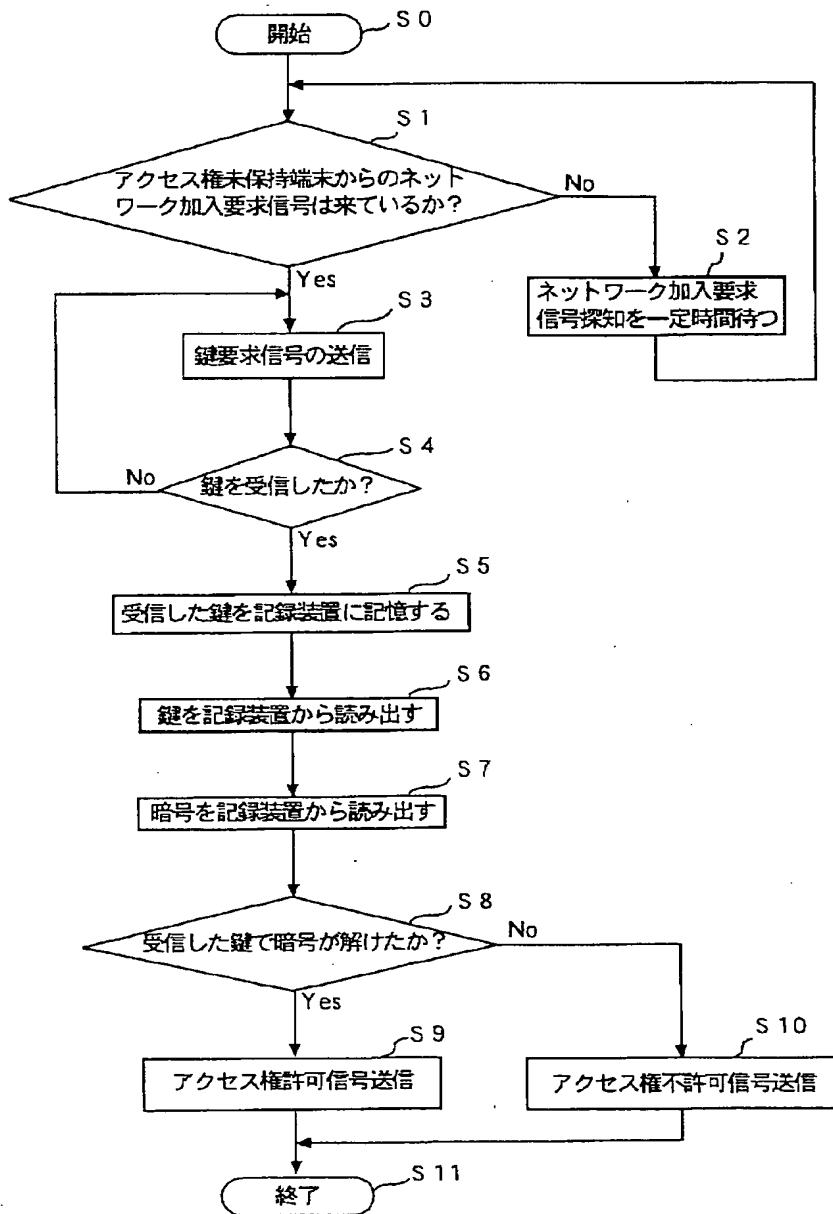
【図3】



【図4】



【図5】



【図6】

アクセス権未保持端末

ネットワーク管理端末

